DISCRETE AND CONTINUOUS
DYNAMICAL SYSTEMS
Volume **13**, Number **2**, July **2005**

Website: http://aimSciences.org

pp. **491–502**

MASTER–SLAVE SYNCHRONIZATION OF AFFINE CELLULAR AUTOMATON PAIRS

Gelasio Salazar, Edgardo Ugalde and Jesús Urías

Instituto de Física, UASLP
Alvaro Obregon 64, San Luis Potosí, SLP, 78000 México

Abstract. Necessary and sufficient conditions are given for master–slave synchronization of any pair of unidirectionally coupled one–dimensional affine cellular automata of rank one. In each case the synchronization condition is expressed in terms of the coupling and the arithmetic properties of the automaton local rule. The asymptotic behavior of finite length affine automata of rank one, subjected to Dirichlet boundary conditions, is shown to be equivalent to the synchronization problem.

1. **Introduction.** The synchronization phenomenon observed in coupled subsystems has been studied extensively for iterated maps and ordinary differential equations. Some rigorous results have been established for those systems already. The synchronization phenomenon has also been observed in several types of interacting extended models.

1. Systems of globally coupled oscillators show a global behavior where all individual oscillators get entrained in periodic orbits [5] when the coupling strength is big enough.
2. Synchronization of spatiotemporally chaotic extended systems has been studied in the context of coupled one–dimensional complex Ginzburg–Landau equations. The coupled pair shows a regime of spatiotemporal intermittency that was described in [1] in terms of the space–time synchronized chaotic motion of localized structures.

However, much less is known about the theoretical basis for the synchronization phenomenon in interacting extended systems. Here we address the problem of master–slave synchronization in coupled one–dimensional cellular automata. Two forms of coupling have been considered in the literature. One is to take a stochastic coupling [11, 2] between automata. The strength of coupling is handled by means of a probability, and numerical evidence in several examples supports the existence of a critical value of the probability above which the pair synchronizes identically. The other form is a deterministic coupling as was done in [10]. Therein, necessary and sufficient conditions for synchronization of coupled affine elementary cellular automata were given. The proof in [10] is based on the existence of a connection between synchronization and nilpotency of matrices. The natural generalization of that approach led us to the study of the nilpotency of a broader class of matrices. The answer to the nilpotency problem allows us to give a definitive answer

2000 *Mathematics Subject Classification.* 15A33, 37B15, 15A90.

Key words and phrases. Cellular automata, Synchronization, Dirichlet boundary conditions, Nilpotency.

to the master–slave synchronization problem in coupled pairs of one–dimensional affine cellular automata of rank one. It also tells us about the asymptotics of time evolution of affine cellular automata subjected to Dirichlet boundary conditions.

In Section 2 the interacting scheme between cellular automata is described and the connection between master–slave synchronization and nilpotency of matrices is established as Lemma 2.1. The main theorem about the nilpotency of matrices over $\mathbb{Z}_k$ is stated in Section 3. Its direct consequence on master–slave synchronization is Theorem 4.1 in Section 4. The implications on the asymptotics of cellular automata under Dirichlet boundary conditions are discussed in Section 5.

All proofs are collected in the Appendices.

2. **Master–slave synchronization.** Consider the finite cyclic ring $\mathbb{Z}_k$ of residual classes modulo k. As usual, we identify the elements of $\mathbb{Z}_k$ with the integers $0, 1, \ldots, k-1$, and denote $a+b$ and ab the operations $a+b$ (mod k) and ab (mod k) respectively. We supply the product space $\mathbb{Z}_k^{\mathbb{Z}}$ with the natural coordinate–wise operations.

A local map $f : \mathbb{Z}_k^3 \to \mathbb{Z}_k$ such that $f(\mathbf{x}_{-1}\mathbf{x}_0\mathbf{x}_1) = a\mathbf{x}_{-1} + b\mathbf{x}_0 + c\mathbf{x}_1 + d$ specifies the affine cellular automaton $F : \mathbb{Z}_k^{\mathbb{Z}} \to \mathbb{Z}_k^{\mathbb{Z}}$ with n–th coordinate given by

$$F(\mathbf{x})_n = f(\mathbf{x}_{n-1}\mathbf{x}_n\mathbf{x}_{n+1}) = a\mathbf{x}_{n-1} + b\mathbf{x}_n + c\mathbf{x}_{n+1} + d, \quad n \in \mathbb{Z} \ . \tag{1}$$

The transformation F is represented in matrix form as

$$F(\mathbf{x}) = \begin{pmatrix} \ddots & \ddots & \ddots & & & & \\ & a & b & c & & & \\ & & a & b & c & & \\ & & & a & b & c & \\ & & & & \ddots & \ddots & \ddots \end{pmatrix} \begin{pmatrix} \vdots \\ \mathbf{x}_{n-1} \\ \mathbf{x}_n \\ \mathbf{x}_{n+1} \\ \vdots \end{pmatrix} + \begin{pmatrix} \vdots \\ d \\ d \\ d \\ \vdots \end{pmatrix} . \tag{2}$$

In the previous equation let the infinite tridiagonal matrix be denoted by M_{abc}, and let $\underline{d} := (\ldots, d, d, d, \ldots)$, $d \in \mathbb{Z}_k$ denote the infinite constant vector.

The forward orbit of the configuration $\mathbf{x} \in \mathbb{Z}_k^{\mathbb{Z}}$ under the action of the transformation F is the sequence $\mathbf{x}$, $\mathbf{x}^1$, …, $\mathbf{x}^t$, …, with

$$\mathbf{x}^t = M_{abc}^t\mathbf{x} + \sum_{j=0}^{t-1} M_{abc}^j \underline{d} \ , \quad t \geq 1 \ . \tag{3}$$

Two cellular automata, $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}$ and $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}'$ in $\mathbb{Z}_k^{\mathbb{Z}}$ (having the same linear part but may have different constant terms, d and $d' \in \mathbb{Z}_k$) are coupled unidirectionally as follows. For $C \in \{0,1\}^{\mathbb{Z}}$, a constant coupling sequence, consider the projection $\Pi_C : \mathbb{Z}_k^{\mathbb{Z}} \to \mathbb{Z}_k^{\mathbb{Z}}$ defined as

$$(\Pi_C\mathbf{x})_i = \begin{cases} \mathbf{x}_i & \text{if } C_i = 1 \\ 0 & \text{otherwise} \end{cases} \ . \tag{4}$$

The extended automaton

$$\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \mapsto \begin{pmatrix} M_{abc}\mathbf{x} + \underline{d} \\ M_{abc}\mathbf{y} + \underline{d}' + \Pi_C\big(M_{abc}(\mathbf{x}-\mathbf{y}) + \underline{d} - \underline{d}'\big) \end{pmatrix} , \tag{5}$$

defines an unidirectionally coupled pair, with coupling sequence C. Notice that for a coupling sequence $C = \underline{0} := (\ldots, 0, 0, 0, \ldots)$ the two subsystems in (5) evolve independently, while for the coupling $C = \underline{1} := (\ldots, 1, 1, 1, \ldots)$ the second subsystem is just a copy of the first one.

The coupled pair (5) synchronizes if the difference between the $\mathbf{x}^t$ and $\mathbf{y}^t$ configurations, $\Delta^t := \mathbf{x}^t - \mathbf{y}^t$, goes in time to a constant configuration $\underline{\delta} \in \mathbb{Z}_k^{\mathbb{Z}}$, i. e., if $\Delta^t \to \underline{\delta}$ as $t \to \infty$, regardless of the initial configurations $\mathbf{x}^0$ and $\mathbf{y}^0$. In this situation we say that the extended automaton (5) is a master–slave pair. The subsystem in (5) that is evolving autonomously is called the master subsystem. The second subsystem is called the slave one since it evolves asymptotically, up to a spatially–homogeneous configuration $\underline{\delta}$, in the same way as the master subsystem does. The synchronization regime known as identical synchronization corresponds to $\Delta^t \to \underline{\delta} = \underline{0}$, the null configuration with all its coordinates equal to zero.

For affine automata the difference Δ^t evolves according to the rule

$$\Delta^{t+1} = \left(\Pi_{\underline{1}-C} M_{abc}\right) \Delta^t + \Pi_{\underline{1}-C}(\underline{d} - \underline{d}'). \tag{6}$$

Thus, *the coupled pair (5) synchronizes* if for any pair $\mathbf{x}^0, \mathbf{y}^0 \in \mathbb{Z}_k^{\mathbb{Z}}$ of initial configurations the difference

$$\Delta^t = \left(M_{abc}^C\right)^{t-1} M_{abc}\Delta^0 + \sum_{j=0}^{t-1} \left(M_{abc}^C\right)^j (\underline{d} - \underline{d}') \quad \to \quad \underline{\delta}, \tag{7}$$

as t tends to infinity, where $M_{abc}^C := \Pi_{\underline{1}-C} M_{abc} \Pi_{\underline{1}-C}$.

The limit $\Delta^t \to \underline{\delta}$ in (7) is supposed to take place with respect to some "natural" metric in $\mathbb{Z}_k^{\mathbb{Z}}$. In order to avoid complications regarding the definition of the metric, from now on we will suppose that the length of a block of consecutive zeros in the coupling sequence C is bounded. For such a coupling sequence C the operator M_{abc}^C has the block–diagonal form

$$M_{abc}^C = \begin{pmatrix} \ddots & & & & & & & \\ & M_{abc,\ell_{i-1}} & & & & & & \\ & & 0 & & & & & \\ & & & M_{abc,\ell_i} & & & & \\ & & & & 0 & & & \\ & & & & & M_{abc,\ell_{i+1}} & & \\ & & & & & & \ddots & \end{pmatrix}. \tag{8}$$

Each block $M_{a,b,c;\ell_i}$ is a $\ell_i \times \ell_i$ submatrix of the form

$$M_{a,b,c;\ell_i} = \begin{pmatrix} b & c & 0 & \cdots & 0 \\ a & b & c & & \vdots \\ & \ddots & \ddots & \ddots & \\ \vdots & & a & b & c \\ 0 & \cdots & 0 & a & b \end{pmatrix}. \tag{9}$$

The 1×1 zero sub–blocks correspond to the coordinates where C is equal to one, while the positive integer numbers ℓ_i, $i \in \mathbb{Z}$, are the lengths of the blocks of consecutive zeros in the coupling sequence C. The evolution of the differences in (7) splits into independent finite blocks. For the i–th block we have that for all $\Delta^0 \in \mathbb{Z}_k^{\mathbb{Z}}$,

$$M_{abc,\ell_i}^t (M_{abc}^C \Delta^0)_{I_i} + \sum_{j=0}^{t} M_{abc,\ell_i}^j (\underline{d} - \underline{d}')_{I_i} \to \underline{\delta}_{I_i}, \tag{10}$$

as $t \to \infty$. Here $I_i \subset \mathbb{Z}$ is the interval of length ℓ_i containing all the coordinates of the sub–matrix M_{abc,ℓ_i}, and $\mathbf{x}_{I_i} \in \mathbb{Z}_k^{I_i}$ denotes the restriction of the configuration

$\mathbf{x}$ to that interval. Since $\mathbb{Z}_k^{I_i}$ is a finite set, the convergence in (10) is in fact the eventual equality

$$M^t_{abc,\ell_i}(M^C_{abc}\Delta^0)_{I_i} + \sum_{j=0}^{t} M^j_{abc,\ell_i}(\underline{d}-\underline{d}')_{I_i} = \underline{\delta}_{I_i}, \tag{11}$$

for all $\Delta^0 \in \mathbb{Z}_k^{\mathbb{Z}}$ (for all sufficiently large t) and each i. Thus, we need no metric in $\mathbb{Z}_k^{\mathbb{Z}}$.

Assume there exists T such that for every $t \geq T$ condition (11) is satisfied. Then, putting $\Delta^0 = \underline{0}$ in (11) shows that $\sum_{j=0}^{t} M^j_{abc,\ell_i}(\underline{d}-\underline{d}')_{I_i} = \underline{\delta}_{I_i}$ for all sufficiently large t and thus,

$$M^t_{abc,\ell_i}(M^C_{abc}\Delta^0)_{I_i} = 0,$$

for all Δ_0 and all $t \geq T$. Given the block–diagonal form (8) of the operator M^C_{abc}, for each block we have

$$M^t_{abc,\ell_i} M_{abc,\ell_i} \Delta^0_{I_i} = 0 \tag{12}$$

for all sufficiently large t. Since the initial difference $\Delta^0_{I_i}$ is arbitrary, the sub–block matrix M_{abc,ℓ_i} has to be nilpotent for condition (12) to hold. The converse follows immediately: if each one of the sub–matrices M_{abc,ℓ_i} in (8) is nilpotent, then the extended automaton (5) synchronizes in the sense of (7).

The results of the present section are summarized in the following.

Lemma 2.1. *The extended automaton (5) is a master–slave pair if and only if the operator $M^C_{abc} := \Pi_{\underline{1}-C} M_{abc} \Pi_{\underline{1}-C}$, having form (8), is nilpotent. When this is the case there exists a least positive $T < \infty$ such that for every $t \geq T$: $\mathbf{y}^t = \mathbf{x}^t - \underline{\delta}$ with $\delta = (d-d')\sum_{j=0}^{T-1}(a+b+c)^j$.*

3. **Result on the nilpotency of matrices.** Lemma 2.1 makes the synchronization problem equivalent to the problem of determining sufficient and necessary conditions for the nilpotency of finite–dimensional tridiagonal matrices $M_{a,b,c;\ell}$ of the form (9) over the finite ring $\mathbb{Z}_k$. The nilpotency problem is solved by the theorem in this section. We are not aware that such a result exists in the literature. Thus, in Appendix 6 we present a detailed proof of Theorem 3.1.

Throughout all that follows, $M_{a,b,c;\ell}$ denotes a $\ell \times \ell$ matrix of the form (9) with entries a, b and c in $\mathbb{Z}_k$.

Theorem 3.1. *Let $k = p_1^{s_1} p_2^{s_2} \cdots p_i^{s_i} \cdots p_m^{s_m}$ with $s_i > 0$ and p_i prime numbers in the order $p_1 < p_2 < \cdots p_i \cdots < p_m$. Then $M_{a,b,c;\ell}$ is nilpotent over $\mathbb{Z}_k$ if and only if*

I) *For each $p_i > 2$, $ac = b = 0 \pmod{p_i}$.*
and
II) *For $p_1 = 2$ one of the following conditions holds*
1. *$ac = b = 0 \pmod 2$, or*
2. *$abc = 1 \pmod 2$ and $\ell = 2$, or*
3. *$ac = 1 \pmod 2$, $b = 0 \pmod 2$ and $\ell \in \{2^n - 1 : \ n \geq 1\}$.*

4. **Result on synchronization.** Theorem 3.1 is translated directly to the following result on master–slave synchronization of coupled pairs of the type (5).

Theorem 4.1. *Let $\mathbb{Z}_k$ be the ring of definition of the extended automaton (5). Let $p_1^{s_1} p_2^{s_2} \cdots p_i^{s_i} \cdots p_m^{s_m}$, $s_i > 0$, be the factorization of k into primes $p_1 < p_2 < \cdots p_i \cdots < p_m$. Then (5) is a master–slave pair if and only if*

I) *For each* $p_i > 2$, $ac = b = 0 \pmod{p_i}$.
and
II) *For* $p_1 = 2$ *one of the following conditions holds*
1. $ac = b = 0 \pmod 2$, *or*
2. $abc = 1 \pmod 2$ *and each* ℓ *in the coupling sequence* C *is* $\ell = 2$, *or*
3. $ac = 1 \pmod 2$, $b = 0 \pmod 2$ *and all the blocks of consecutive zeros in the coupling sequence* C *have lengths in the set* $\{2^n - 1 : \ n \geq 1\}$.

5. **Concluding Remarks.**

5.1. **Affine cellular automata of higher rank.** In this case the synchronization problem cannot be reduced in general to a problem of nilpotency of $(2r+1)$–diagonal matrices over the ring $\mathbb{Z}_k$. Only for very particular coupling sequences is it possible to decompose the dynamics of the difference between the automaton configurations into finite dimensional blocks.

5.2. **Strength of coupling and synchronization.** It is reasonable to expect that coupled subsystems synchronize in a master–slave regime when the coupling sequence C is close to the homogeneous configuration $\underline{1}$.

Let $\{\ell_i : \ i \in \mathbb{Z}\}$ be the sequence of lengths of the blocks of zeros in C. If C is such that

$$\epsilon(C) := 1 - \lim_{N\to\infty} \frac{2N+1}{\sum_{i=-N}^{N}(\ell_i + 1)}$$

exists, then closeness of C to $\underline{1}$ is measured by $\epsilon(C)$ and we may call it the strength of coupling configuration C. By analogy to the continuous mapping case, we would expect a transition from non–synchronization to full synchronization as $\epsilon(C)$ approaches 1. However, Theorem 4.1 implies this criterion is not relevant for coupled CA.

As an example, consider the automata $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}$ and $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}'$ in $\mathbb{Z}_{2p^s}^{\mathbb{Z}}$ such that $(a,b,c)_2 = (1,0,1)$, and $(a,b,c)_p = (a,0,c)$, with ac zero or a divisor of zero modulo p^s. Let us remind that $(a,b,c)_q$ denotes the triple $(a(\mathrm{mod}\, q)$, $b(\mathrm{mod}\, q)$, $c(\mathrm{mod}\, q))$. If the automata are coupled by means of a coupling sequence C, each of its zero blocks having length $\ell_i = 2^{n_i} - 1$ for some n_i, then the coupled pair synchronizes. Notice that the coupling strengths $\epsilon(C)$ may have any value in $[0,1]$ by using coupling configurations C of this kind. For this note that if $\{\ell_i = 2^{n_i} - 1 : \ i \in \mathbb{Z}\}$ are the lengths of the zero blocks in C, then $\epsilon(C) = \lim_{N\to\infty}(2N+1)/(\sum_{i=-N}^{N} 2^{n_i})$.

So, in the example there is no transition from non–synchronization to full synchronization as we move the coupling strength $\epsilon(C)$ along the full range $(0,1)$. As far as we use a coupling configuration with zero blocks of lengths $\ell_i = 2^{n_i} - 1$ the pair will always synchronize.

Thus a strong coupling strength is not a necessary condition for synchronization.

On the other hand, for automata $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}$ and $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}'$ in $\mathbb{Z}_p^{\mathbb{Z}}$ with $p > 2$ a prime number and $ac \neq 0$, the only coupling constant for which the coupled pair synchronizes is $C = \underline{1}$. For any other coupling, the finite matrices associated to the blocks of consecutive zeros are not nilpotent.

Hence, for the class of cellular automata here considered, the synchronization phenomenon is not controlled by the strength of the coupling but by the arithmetic properties of the local rule specifying the cellular automata in the coupled pair.

5.3. **Dynamics under Dirichlet boundary conditions.** In computer simulations we can only consider finite versions of a given cellular automaton, and try to extrapolate to the behavior of the infinite automaton by taking large finite versions. This approach presumes that finite versions converge in some sense to the infinite cellular automaton.

The finite versions of a cellular automaton are obtained by imposing boundary conditions. The Dirichlet boundary conditions force the configurations to be zero everywhere outside a window of finite length ℓ. Denote $\mathbf{y}_{[0,N-1]}$ the restrictions to the interval $[0, N-1]$, of the configuration $\mathbf{y} \in \mathbb{Z}_k^{\mathbb{Z}}$. The dynamics of the affine automaton $F(\mathbf{x}) = M_{abc}\mathbf{x} + \underline{d}$, when subjected to Dirichlet boundary conditions inside the finite window $[0, N-1]$, is determined by

$$\mathbf{x}^t_{[0,N-1]} = M^t_{abc,N}\mathbf{x}_N + \sum_{j=0}^{t-1} M^j_{abc,N}\underline{d}_{[0,N-1]} \ . \tag{13}$$

A trivial asymptotic behavior of the automaton subjected to Dirichlet boundary conditions is equivalent to the nilpotency of the finite matrix determining the dynamics. The following is proved in Appendix 7.

Lemma 5.1. *The forward orbit of every initial configuration goes, under Dirichlet boundary conditions, to a fixed point in finite time if and only if matrix $M_{abc,N}$ is nilpotent.*

5.4. **Thermodynamic limit.** One would like to relate the behavior of finite versions of a cellular automaton, that we obtain by imposing Dirichlet boundary conditions, to the behavior of the infinite automaton. One way to do this is to compare different finite versions. A limit behavior would exist if large finite versions behave more similar one to the other as their sizes become larger. Suppose that to each finite version of the automaton we associate a natural invariant measure. Then we would say that two finite versions behave similarly if their corresponding natural invariant measures are close in some metric. Then a thermodynamic limit could be attained if larger finite versions have more similar invariant measures. On the other hand, if the asymptotic invariant sets of the finite versions do not have a limit behavior, such thermodynamic limit cannot exist. Next we give an example.

Let p be an odd prime and $s \geq 0$. Consider an affine cellular automata $\mathbf{x} \mapsto M_{abc}\mathbf{x} + \underline{d}$ in $\mathbb{Z}_{2p^s}^{\mathbb{Z}}$ such that $(a, b, c)_2 = (1, 0, 1)$, and $(a, b, c)_p = (a, 0, b)$ with $ac = 0$ or a divisor of zero modulo p^s. Theorem 3.1 ensures that $M_{a,b,c;\ell}$ is nilpotent for all sizes $\ell = 2^n - 1$, and only for these sizes. This means that for infinitely many sizes, the asymptotic behavior of the automaton $\mathbf{x} \mapsto M_{a,b,c;\ell}\mathbf{x} + \underline{d}$ subjected to Dirichlet boundary conditions is trivial, in the sense that all initial conditions evolve to a unique fixed point. In this situation, the natural invariant measure is a Dirac measure concentrated in this unique fixed point. On the other hand infinite size behavior cannot be trivial, because for infinitely many lengths the invariant limit set has more than one point. It is in fact a finite collection of long periodic orbits. Thus, there cannot be a thermodynamic limit for the class of affine cellular automata described above.

5.5. **Invariant measures.** There are few works concerning the statistical behavior of cellular automata. It was proven in [4, 9] that for a certain class of one–dimensional cellular automata, which includes some of the affine examples, the uniform measure is invariant. Whether this measure can be obtained as a thermodynamic limit of uniform invariant measures of finite automata is unknown. There

are some studies on the limit behavior of measures under the action of the automaton dynamics [3, 6, 8], and probably the technique therein developed can be useful a tool to deal with the thermodynamic limit problem. As we have shown in this paper, the limit does not exist in general, but it could exist for particular families of cellular automata, such as affine cellular automata on a prime alphabet.

5.6. **Applications.** Synchronization of cellular automata has been applied to device a pseudorandom number generator that is asymptotically perfect [7]. It is wired as a digital system that is fast and small, with potential applications to cryptography.

6. **Appendix: Proof of Theorem 3.1.** The proof follows three main steps. The first one is to prove that an integer matrix on $\mathbb{Z}_{pq}$, with p and q relatively prime, is nilpotent if and only if it is nilpotent over $\mathbb{Z}_p$ and over $\mathbb{Z}_q$. This is Proposition 6.1 below, that reduces the nilpotency problem to prove it for integer matrices $M_{a,b,c;\ell}$ over $\mathbb{Z}_{p^s}$, with p a prime number and positive s. In the second step, Lemma 6.1, it is proved that an integer matrix is nilpotent over $\mathbb{Z}_{p^s}$ if and only if it is nilpotent over $\mathbb{Z}_p$. This reduces the problem to give necessary and sufficient conditions for nilpotency of an integer matrix $M_{a,b,c;\ell}$ over $\mathbb{Z}_p$, p a prime number. This is done in Proposition 6.2 below. This concludes step three and the proof of Theorem 3.1.

Proposition 6.1. *Let the integers $p > 0$ and $q > 0$ be relatively prime. Let M be a $\ell \times \ell$ matrix with entries in $\mathbb{Z}_{pq}$. Then $M^n = 0 \pmod{pq}$ for some $n > 0$ if and only if $\big(M^n = 0 \pmod{p}\big)$ and $\big(M^n = 0 \pmod{q}\big)$ for the same value of n.*

Proof. For $k = pq$ with $(p, q) = 1$, the transformation

$$r \pmod{k} \leftrightarrow (r \bmod p, r \bmod q)$$

is a ring isomorphism between $\mathbb{Z}_k$ and $\mathbb{Z}_p \times \mathbb{Z}_q$. This isomorphism induces in a natural way another one between the ring $\mathcal{M}_\ell(\mathbb{Z}_k)$ of $\ell \times \ell$ matrices over $\mathbb{Z}_k$ and the ring $\mathcal{M}_\ell(\mathbb{Z}_p) \times \mathcal{M}_\ell(\mathbb{Z}_q)$. The proposition then follows. □

Thus, the nilpotency of $M_{a,b,c;\ell}$ over $\mathbb{Z}_k$ ($(a, b, c) \in \mathbb{Z}_k^3$) with a composite integer number $k = pq$ and $(p, q) = 1$ is determined by the nilpotency of its projections $M_{(a,b,c)_p;\ell}$ over $\mathbb{Z}_p$ and $M_{(a,b,c)_q;\ell}$ over $\mathbb{Z}_q$. Here $(a, b, c)_p$ denotes the triple obtained reducing modulo p each of a, b and c (similarly for $(a, b, c)_q$): $M_{(a,b,c)_{pq};\ell}$ is nilpotent if and only if both $M_{(a,b,c)_p;\ell}$ and $M_{(a,b,c)_q;\ell}$ are.

This first result tells us that in order to decide about the nilpotency of any tridiagonal matrix over cyclic rings it suffices to prove nilpotency of matrices on rings with order the power of a prime number.

Lemma 6.1. *Let M be a $\ell \times \ell$ integer matrix. Let p be a prime number. Then, for $s > 1$, $M^n = 0 \pmod{p^s}$ for some n if and only if $M^k = 0 \pmod{p}$ for some k.*

Proof. It is evident that $M^n = 0 \pmod{p^s}$ implies $M^n = 0 \pmod{p}$. Assume next that $M^k = 0 \pmod{p}$ for some k. Then there is an integer matrix Q such that $M^k = pQ$. Thus $M^n = 0 \pmod{p^s}$ with $n = ks$. □

The proof of the following Proposition requires several technical lemmas that are collected and proved in Appendix 8.

Proposition 6.2. *Let matrix $M_{a,b,c;\ell}$ have entries in $\mathbb{Z}_p$, with p a prime number. Then the following hold.*

I) *For $p > 2$ the matrix $M_{a,b,c;\ell}$ is nilpotent if and only if $ac = b = 0 \pmod{p}$.*
II) *For $p = 2$ the matrix $M_{a,b,c;\ell}$ is nilpotent if and only if one of the following conditions holds.*

1. $ac = b = 0 \pmod 2$.
2. $abc = 1 \pmod 2$ *and* $\ell = 2$.
3. $(a, b, c) = (1, 0, 1) \pmod 2$ *and* $\ell \in \{2^n - 1 : \ n \geq 1\}$.

Proof of Proposition 6.2 I). Proceeds by discrimination of cases.
Case $ac = b = 0 \pmod p$. If $c \neq 0$, then, by Lemma 8.1–(6), $M^n_{a,b,c;\ell} = 0$ for $n \geq \ell$. Otherwise, if $a \neq 0$, by Lemma 8.1–(1) and 8.1–(6), the same conclusion holds.

Let $P_\ell(\lambda) = \lambda^\ell + q^\ell_{\ell-1}\lambda^{\ell-1} + \cdots q^\ell_1\lambda + q^\ell_0$ be the characteristic polynomial of matrix $M_{a,b,c;\ell}$. Because of Lemma 8.3, for the rest of cases it is enough to prove that $P_\ell(\lambda) \neq \lambda^\ell$.
Consider first the case of triples (a, b, c) with $ac \neq 0$ and $b = 0$. Lemma 8.4 tells us that

$$\begin{aligned} P_{2m} &= \sum_{j=0}^{m} \binom{2m-j}{j} \lambda^{2(m-j)}(-ac)^j, \\ P_{2m+1} &= \sum_{j=0}^{m} \binom{2m+1-j}{j} \lambda^{2(m-j)+1}(-ac)^j, \end{aligned}$$

for all $m \in \mathbb{N}$. Thus, in the case of an even $\ell = 2m$ the constant term $q^{2m}_0 = (-ac)^m$ is not null, and this solves the problem for all even ℓ. In the case of odd ℓ, the coefficients $q^{2m+1}_1 = (m + 1)(-ac)^m$ and $q^{2m+1}_{2m-1} = 2m(-ac)$ in P_{2m+1} are not a multiple of the prime number $p > 2$, simultaneously. Here concludes the case $ac \neq 0$ and $b = 0$.

Next case consists of triples (a, b, c) with both $ac \neq 0$ and $b \neq 0$. A direct computation of coefficient $q^\ell_{\ell-1}$ of the characteristic polynomial in Lemma 8.4 yields $q^\ell_{\ell-1} = -\ell b$ that is not zero whenever ℓ is not a multiple of p. Similarly, in the case that ℓ is divisible by p, Lemma 8.4 yields $q^\ell_{\ell-2} = -(\ell - 1)ac \neq 0$. Thus, $P_\ell(\lambda) \neq \lambda^\ell$ for every ℓ.

The last case to consider is that of triples $(a, b, c) \in \mathbb{Z}^3_p$ with $ac = 0$ and $b \neq 0$. By Lemma 8.4 we have that $P_\ell(\lambda) = (\lambda - b)^\ell$. □

Proof of Proposition 6.2 II).
For $(a, b, c) = (1, 0, 1)$ the characteristic polynomial (18) is

$$P_\ell(\lambda) = \sum_{j=0}^{\lfloor \ell/2 \rfloor} \binom{\ell - j}{j} \lambda^{\ell-2j}, \tag{14}$$

with coefficients modulo–2 integer numbers. It is clear that for an even ℓ the coefficient $q^\ell_0 = 1$. Thus $P_\ell(\lambda) \neq \lambda^\ell$, and by Lemma 8.3 $M_{a,b,c;\ell}$ is not nilpotent. For ℓ an odd number we consider separately the cases $\ell = 2^n - 1$ and $\ell = 2^n - r$ with $1 < r < 2^{n-1}$ an odd number.

Consider first $\ell = 2^n - 1$. All binomial coefficients in (14) are even for $j > 0$ and then $P_\ell(\lambda) = \lambda^\ell$. This we prove as follows. For $j = 1$ the binomial coefficient in (14) is an even number. For the rest of values $j = 2, 3, \ldots, 2^{n-1} - 1$ we have

$$\binom{\ell - j}{j} = \frac{2}{j} \times \binom{\ell - j}{j - 1} \times \left(2^{n-1} - j\right). \tag{15}$$

Consider first the case j is an odd integer. Since the binomial (15) is an integer number then j divides the product

$$\binom{\ell - j}{j - 1} \times \left(2^{n-1} - j\right)$$

and the binomial (15) is an even number. Next, consider binomial (15) with $j = 2^s r$, $r \geq 1$ an odd integer number and $n-1 > s > 0$. Again by integrality of binomial (15), the odd number r divides the factor

$$\binom{\ell - j}{j-1} \times \left(2^{n-s-1} - r\right)$$

and the binomial (15) happens to be an even number.

It remains the case $\ell = 2^n - r$ with $1 < r < 2^{n-1}$ odd. If $r = 4m+3$ for some $m \in \mathbb{Z}^+$, then

$$q_1^\ell = \binom{2^n - r - (2^{n-1} - \frac{r+1}{2})}{2^{n-1} - \frac{r+1}{2}} = 2^{n-1} - \frac{r-1}{2} = \left(2^{n-1} - 2m\right) + 1,$$

which is an odd number. For $r = 4m+1$, let $m = 2^{s-1}k$ with k an odd number. In this case, for $j = 2^{s-1}$ we have

$$\binom{2^n - r - j}{j} = \binom{2^{s-1}(2(2^{n-s} - k) - 1) - 1}{2^{s-1}} \ , \tag{16}$$

which is always an odd number. Thus $P_\ell(\lambda)$ has at least two non–zero coefficients.

For triples $(a,b,c) = (1,1,0)$ or $(0,1,1)$, by Lemma 8.4, $P_\ell(\lambda) = (\lambda - 1)^\ell$.

For $(a,b,c) = (1,1,1)$ we use the recurrence relation (19) in Lemma 8.4 with initial polynomials $P_0(\lambda) = 1$ and $P_1(\lambda) = \lambda + 1$. The next polynomial is $P_2(\lambda) = \lambda^2$. We remark that the coefficients of all polynomials are taken modulo 2.

Then, relation (19) implies that the independent coefficients q_0^ℓ satisfy the recurrence $q_0^{\ell+2} = q_0^{\ell+1} + q_0^\ell$ with the initial conditions $q_0^0 = q_0^1 = 1$. Thus we obtain

$$q_0^\ell = \begin{cases} 0 & \text{if } \ell = 2 \ (\bmod\ 3) \\ 1 & \text{otherwise.} \end{cases}$$

Similarly, relation (19) implies the recurrence $q_{\ell+1}^{\ell+2} = q_\ell^{\ell+1} + q_{\ell-1}^\ell + 1$ with initial values $q_0^1 = 1$, $q_1^2 = 0$, which give

$$q_{\ell-1}^\ell = \begin{cases} 1 & \text{if } \ell = 1 \ (\bmod\ 3) \\ 0 & \text{otherwise.} \end{cases}$$

Thus, except for $\ell = 2$, the minimal polynomial of $M_{a,b,c;\ell}$ is not λ^ℓ. □

7. **Appendix: Proof of Lemma 5.1.** Assume that $M_{abc,N}^s = 0$ for some $s \in \mathbb{N}$. Then

$$\mathbf{x}_{[0,N-1]}^t = \sum_{j=0}^{s-1} M_{abc,N}^j \underline{d}_{[0,N-1]} \ ,$$

for all $t \geq s$. Conversely, if the forward orbit of every configurations converges to a single fixed point, then $M_{abc,N}$ has to be nilpotent. To see this notice that if $\mathbf{x}_{[0,N-1]}^t = \mathbf{w}_{[0,N-1]}^*$ for each $\mathbf{x}_{[0,N-1]} \in \mathbb{Z}_k^{[0,n-1]}$ and $t \geq s$, according to equation (13)

$$\begin{aligned} \mathbf{w}_{[0,N-1]}^* &= M_{abc,N}^s 0 + \sum_{j=0}^{s-1} M_{abc}^j \underline{d}_{[0,N-1]}, \\ &= M_{abc,N}^s \mathbf{x}_{[0,N-1]} + \sum_{j=0}^{s-1} M_{abc}^j \underline{d}_{[0,N-1]}, \end{aligned}$$

and from this $M_{abc}^s \mathbf{x}_{[0,N-1]} = 0$. □

8. **Appendix: Technical lemmas.** All technicalities needed to prove the nilpotency theorem about the matrices

$$M^n_{a,b,c;\ell} = (M_{a,0,c;\ell} + b\mathbb{1})^n = \sum_{k=0}^{n} \binom{n}{k} M^k_{a,0,c;\ell} b^{n-k} \tag{17}$$

are collected in a series of lemmas.

Lemma 8.1. *Let $M_{a,b,c;\ell}$ be a tridiagonal matrix as in (9). Denote its entries as $M_{a,b,c;\ell}(i,j)$ with $i,\, j = 0,\, \ldots,\, \ell-1$. Then,*

1. *For every positive integer number n, $M^n_{a,b,c;\ell}(i,j) = M^n_{c,b,a;\ell}(j,i)$.*
2. *When $b = 0$, for every $n > 0$*

$$M^n_{a,0,c,;\ell}(i,j) = \begin{cases} 0, & n+j-i = 1 \ (mod\ 2) \\ M^n_{1,0,1;\ell}(i,j) a^{(n-(j-i))/2} c^{(n+(j-i))/2}, & n+j-i = 0 \ (mod\ 2) \end{cases}$$

3. *For $0 < n \le (\ell-1)/2$*

$$M^n_{1,0,1;\ell}(i,j) = \begin{cases} \binom{n}{(n+j-i)/2}, & \text{for } i \ge 0 \text{ and } 1 \le n \le j \le \ell - n - 1 \\ \binom{n}{(n+i-j)/2}, & \text{for } j \ge 0 \text{ and } 1 \le n \le i \le \ell - n - 1 \end{cases}$$

   for $n+j-i = 0$ (mod 2) and $M^n_{1,0,1;\ell}(i,j) = 0$ otherwise.
4. *$M^n_{a,b,c;\ell}(i,j) = 0$ whenever $|j-i| > n$.*
5. *When $a = 0$, then for every $n > 0$*

$$M^n_{0bc}(i,j) = \begin{cases} \binom{n}{j-i} c^{j-i} b^{n-j+i}, & \text{if } \ 0 \le j-i \le n \\ 0, & \text{otherwise} \end{cases} .$$

6. *When $a = b = 0$*

$$M^n_{0,0,c}(i,j) = \begin{cases} c^{j-i}, & n = j-i \\ 0, & n \ne j-i \end{cases} .$$

Proof.
Statement (1) follows by induction in n.
(2) The case $n = 1$ is verified by direct substitution of the matrices $M_{a,0,c;\ell}$ and $M_{1,0,1;\ell}$. For integer numbers $i,\, j = 0,\, 1,\, \ldots,\, \ell-1$ and $n > 1$ assume that

$$M^n_{a,0,c;\ell}(i,j) = M^n_{1,0,1;\ell}(i,j) a^{(n+i-j)/2} b^{(n-i+j)/2} \quad \text{whenever } n+j-i = 0 (\text{mod } 2)$$

and $M^n_{a,0,c;\ell}(i,j) = 0$ otherwise. Then

$$\begin{aligned} M^{n+1}_{a,0,c;\ell}(i,j) &= \sum_{k=0}^{\ell-1} M^n_{a,0,c;\ell}(i,k) M_{a,0,c;\ell}(k,j) \\ &= c M^n_{a,0,c;\ell}(i,j-1) + a M^n_{a,0,c;\ell}(i,j+1) \\ &= a^{(n+1+i-j)/2} c^{(n+1-i+j)/2} \big(M^n_{1,0,1;\ell}(i,j-1) + M^n_{1,0,1;ell}(i,j+1) \big) \\ &= M^n_{1,0,1;\ell}(i,j) a^{(n+1+i-j)/2} c^{(n+1-i+j)/2} \end{aligned}$$

whenever $n+1+j-i = 0$ (mod 2) and $M^{n+1}_{a,0,c;\ell}(i,j) = 0$ otherwise.
(3) Let $e_0 = (1,0,0,\ldots)$, $e_1 = (0,1,0,\ldots)$, $\ldots$ be orthonormal vectors. Then $M_{1,0,1;\ell} e_j = e_{j-1} + e_{j+1}$ for $j \ge 1$. For arbitrarily large ℓ one proves by induction that

$$M^n_{1,0,1;\ell} e_j = \sum_{k=0}^{n} \binom{n}{k} e_{j+n-2k} \ , \quad j \ge n \ .$$

Identifying $M^n_{1,0,1;\ell}(i,j) = \big(e_i,\, M^n_{1,0,1;\ell} e_j\big)$ the result follows for $j \geq n$. Here, (x, y) denotes the scalar product of vectors x and y. By (1) the result follows for $i \geq n$ too.
(4) is a direct consequence of (3), (2) and the binomial expansion (17).
(5) For $m < 0$ let $e_m = (0,\, 0,\, 0,\, \ldots)$. Then, one proves by induction that

$$M^n_{0,b,c;\ell} e_j = \sum_{k=0}^{n} \binom{n}{k} e_{j-k} c^k b^{n-k} \ .$$

Identifying $M^n_{0,b,c;\ell}(i,j) = \big(e_i,\, M^n_{0,b,c;\ell} e_j\big)$ the result follows.
Proof of (6) follows similar steps as the proof of (5). □

The index of a nilpotent matrix N is the smallest positive integer ν such that $N^\nu = 0$. The following result is a corollary of Lemma 8.2 and Lemma 8.3.

Proposition 8.1. *If $M_{a,b,c;\ell}$ is nilpotent then it has index $\nu \leq \ell$. Equality holds when ac is neither zero nor a divisor of zero in $\mathbb{Z}_k$.*

Lemma 8.2. *Let $k \geq 2$ and $(a, b, c) \in \mathbb{Z}_k^3$. Assume ac is neither zero nor a divisor of zero. Then, $M^n_{a,b,c;\ell} \neq 0$ for all $0 < n < \ell$.*

Proof. It is easy to verify that $M^n_{a,b,c;\ell}(0,t) = c^n$ and $M^n_{a,b,c;\ell}(\ell-1, \ell-(n+1)) = a^n$, for all $1 \leq n < \ell$. Assume ac is not zero neither a divisor of zero. Then either $a^n \neq 0$ for all $n \in \mathbb{N}$ or $c^n \neq 0$ for all $n \in \mathbb{N}$. Hence, $M^n_{a,b,c;\ell} \neq 0$ for all $0 < n < \ell$. □

Lemma 8.3. *Let $k \geq 2$ and $(a, b, c) \in \mathbb{Z}_k^3$. Then $M_{a,b,c;\ell}$ is nilpotent if and only if it has characteristic polynomial $P(\lambda) = \lambda^\ell$.*

Proof. By the Hamilton–Cayley theorem, the characteristic polynomial of $M_{a,b,c;\ell}$ is annihilating for $M_{a,b,c;\ell}$. Then, if $P(\lambda) = \lambda^\ell$, we necessarily have $M^\ell_{a,b,c;\ell} = 0$.

On the other hand, each annihilating polynomial is divisible by the minimal one. If $M_{a,b,c;\ell}$ is nilpotent then there is an annihilating monomial which is divisible by the minimal polynomial. Then, the minimal polynomial is also a monomial λ^j with $1 \leq j \leq \ell$. Finally, by the previous Lemma 8.2, $M^j_{a,b,c;\ell} \neq 0$ whenever $1 \leq j < \ell$, implying that the minimal monomial and the characteristic one have same degree ℓ. Then $P(\lambda) = \lambda^\ell$. □

Lemma 8.4. *For fixed $(a, b, c) \in \mathbb{Z}_k^3$ consider the sequence $(M_{a,b,c;\ell})_{\ell \in \mathbb{N}}$. For each $\ell \in \mathbb{N}$ the characteristic polynomial of $M_{a,b,c;\ell}$ is*

$$P_\ell(\lambda) = \sum_{j=0}^{\lfloor \ell/2 \rfloor} \binom{\ell - j}{j} (\lambda - b)^{\ell - 2j} (-ac)^j \ . \tag{18}$$

Moreover, characteristic polynomials satisfy the recurrence relation

$$P_\ell(\lambda) = (\lambda - b) P_{\ell-1}(\lambda) - ac P_{\ell-2}(\lambda) \ , \tag{19}$$

starting with $P_1(\lambda) = \lambda - b$ and $P_2(\lambda) = (\lambda - b)^2 - ac$.

Proof. Polynomial (18) is obtained by considering the following definition

$$\det(\lambda \mathbb{I} - M_{a,b,c;\ell}) = \sum_{\rho \in S_\ell} \epsilon(\rho) \prod_{j=0}^{\ell-1} \big[\lambda \mathbb{I} - M_{a,b,c;\ell}\big](j, \rho(j)) \ , \tag{20}$$

where the sum is over all permutations ρ of $(0, 1, \ldots, \ell-1)$ and $\epsilon(\rho)$ is the sign of the permutation. Each permutation can be expressed as a composition of transpositions of the kind $(i+1, 1)$. The product $(\lambda - b)^{\ell-2j}(ac)^j$ appears in (20) for permutations

ρ consisting of j transpositions each, having sign $\epsilon(\rho) = (-1)^j$. Each one of such permutations corresponds to a choice of j elements from a set of cardinality $\ell - j$. In this way polynomial (18) follows.

The recurrence relation (19) results if we consider the recursive definition of the determinant instead. □

REFERENCES

[1] A. Amengual, E. Hernández–García, R. Montagne and M. San Miguel, *Synchronization of spatiotemporal chaos: The regime of coupled spatiotemporal intermittency*. Phys. Rev. Letters **78** (1997) 4379–4382.

[2] F. Bagnoli and R. Rechtman, *Synchronization and maximum Lyapunov exponents of cellular automata*. Phys. Rev. E **59** (1999) R1307–R1310.

[3] F. Blanchard and P. Tisseur, *Some properties of cellular automata with equicontinuity points*. Ann. Inst. Henri Poincaré, Probabilité et Statistique **35** (2000) 569–582.

[4] F. Blanchard and A. Maass, *Dynamical properties of expansive one–sided cellular automata*. Israel J. Math. **99** (1997) 149–174.

[5] Y. Kuramoto, Chemical oscillations, waves and turbulence. Springer, Berlin (1984).

[6] A. Maass and S. Martínez, *On Cesàro limit distribution of a class of permutative cellular automata*. J. Stat. Phys. **90** (1998) 435–458.

[7] M. Mejía and J. Urías, *An asymptotically perfect pseudorandom generator*. Discrete and Continuous Dynamical Sys. **7** (2001) 115–126.

[8] M. Pivato and R. Yassawi, *Limit measures for affine cellular automata*. Ergod. Th. & Dynam. Sys. (2002), 22, 1269–1287.

[9] M. A. Shereshevsky, *Ergodic properties of certain surjective cellular automata*. Monatshefte für Mathematik **114** (2000) 305–316.

[10] J. Urías, G. Salazar and E. Ugalde, *Synchronization of cellular automaton pairs*. Chaos **8** (1998) 814–818.

[11] D.H. Zanette and L.G. Morelli, *Synchronization of coupled extended dynamical systems: a short review*. Intl. J. Bifurcation and Chaos **13** (2003) 781–796.

Received October 2004; revised April 2005

E-mail address: [gsalazar, ugalde, jurias]@ifisica.uaslp.mx